**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims**

Claim 1 (Currently Amended): A computer system for scanning ~~for malware~~ a computer file including ~~containing~~ source code of a computer program in a given computer language for malware, the system comprising:

means for separating the source code into groups of constituent parts, each group comprising parts of a ~~corresponding to~~ different type of structural part ~~parts~~ of the program;

means for processing each group ~~part~~ to count the number of occurrences in that group ~~part~~ of characters of a character set to obtain a frequency distribution of characters in that group ~~part~~;

means for comparing the character frequency distribution of each group ~~part~~ with an expected range of frequency distributions; and

means for flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means.

Claim 2 (Currently Amended): A system according to claim 1, wherein the flagging means is operative to flag the file as suspect if the comparing means detects that the frequency distribution of one or more of said groups ~~parts~~ does not match an expected range.

Claim 3 (Currently Amended): A system according to claim 1, wherein the flagging means is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each group ~~part~~ with an expected frequency distribution.

Claim 4 (Currently Amended): A system according to claim 1, wherein, in operation of the comparing means, the range of distributions considered ~~which it considers~~ as representing an acceptable match for the group ~~part~~ is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

Claim 5 (Currently Amended): A system according to claim 1, further comprising ~~and including~~:

means for maintaining an exception list of files which by their contents are to be treated as exceptions;

means for identifying a file as being included in the exception list; and

wherein a file is not marked as suspect if it is identified as being on the exception list.

Claim 6 (Currently Amended): A system according to claim 1, wherein duplicates of constituent parts are ignored.

Claim 7 (Currently Amended): A method for scanning ~~for malware~~ a computer file including ~~containing~~ source code of a computer program in a given computer language for malware, the method comprising:

separating the source code into groups of constituent parts, each group comprising parts of a ~~corresponding to~~ different type of structural part ~~parts~~ of the program;

processing each group ~~part~~ to count the number of occurrences in that group ~~part~~ of characters of a character set to obtain a frequency distribution of characters in that group ~~part~~;

comparing the character frequency distribution of each group ~~part~~ with an expected range of frequency distributions; and

flagging the file as suspect or not depending on the result of one or more comparisons by the comparing ~~means~~.

Claim 8 (Currently Amended): A method according to claim 7, wherein the flagging ~~means~~ is operative to flag the file as suspect if the comparing ~~means~~ detects that

the frequency distribution of one or more of said groups ~~parts~~ does not match an expected range.

Claim 9 (Currently Amended): A method according to claim 7, wherein the flagging ~~means~~ is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each group ~~part~~ with an expected frequency distribution.

Claim 10 (Currently Amended): A method according to claim 7, wherein, in ~~operation of~~ the comparing ~~means~~, the range of distributions which is considered ~~it considers~~ as representing an acceptable match for the group ~~part~~ is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

Claim 11 (Currently Amended): A method according to claim 7, further comprising ~~and including~~:

maintaining an exception list of files which by their contents are to be treated as exceptions;

identifying a file as being included in the exception list; and

wherein a file is not marked as suspect if it is identified as being on the exception list.

Claim 12 (New): A system according to claim 1, wherein the groups comprise at least one of a group of comments, a group of variable names, a group of subroutine names, and a group of strings.

Claim 13 (New): A method according to claim 7, wherein duplicates of constituent parts are ignored.

Claim 14 (New): A method according to claim 7, wherein the groups comprise at least one of a group of comments, a group of variable names, a group of subroutine names, and a group of strings.

Claim 15 (New): A computer readable medium having stored thereon instructions for causing a computer to carry out a method for scanning a computer file including source code of a computer program in a given computer language for malware, the method comprising:

separating the source code into groups of constituent parts, each group comprising parts of a different type of structural part of the program;

processing each group to count the number of occurrences in that group of characters of a character set to obtain a frequency distribution of characters in that group;

comparing the character frequency distribution of each group with an expected range of frequency distributions; and

flagging the file as suspect or not depending on the result of one or more comparisons by the comparing.

Claim 16 (New): A system comprising a computer-readable medium according to claim 15.